REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
15-05-2014

2. REPORT TYPE
FINAL

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
"Can't stop the signal": Regaining reliable access to cyberspace

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Michael Pyne, LT, USN

Paper Advisor (if Any): **N/A**

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
For Example: Distribution Statement A: Approved for public release; Distribution is unlimited. Reference: DOD Directive 5230.24

13. SUPPLEMENTARY NOTES A paper submitted to the Naval War College faculty in partial satisfaction of the requirements of the Joint Military Operations Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

Operational commanders of modern militaries increasingly rely on access to cyberspace, directly or indirectly, to perform a wide variety of required operational functions, including command and control.

As access to cyber becomes more of a "force multiplier" for operational forces, it also becomes a critical vulnerability to those forces. At the same time, many current concepts and plans for operating in anti-access and area-denial environments depend on reliable access to cyberspace. However, some of the nations most able to deny allied forces access to an operational environment also may be able to deny access to the satellites currently underpinning access to cyber.

This paper proposes ensuring reliable access to cyber for command and control by developing operational procedures to utilize unmanned airborne relays. In addition the other operational benefits that would follow from the use of relays are examined, including a more credible deterrence capability and benefits to intelligence collection, reconnaissance, and tactical-level actions.

15. SUBJECT TERMS
Command and control; C2 Organization; Network-Centric Warfare; Cyberspace Access

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON** Chairman, JMO Dept
a. REPORT UNCLASSIFIED	**b. ABSTRACT** UNCLASSIFIED	**c. THIS PAGE** UNCLASSIFIED		**24**	**19b. TELEPHONE NUMBER** *(include area code)* 401-841-3556

NAVAL WAR COLLEGE
Newport, R.I.

“Can’t stop the signal”: Regaining reliable access to cyberspace for command and control

by

Michael Pyne

Lieutenant, United States Navy

A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: /s/______________

14 May 2014

Contents

Paper Abstract

Operational commanders of modern militaries increasingly rely on access to cyberspace, directly or indirectly, to perform a wide variety of required operational functions, including command and control.

As access to cyber becomes more of a “force multiplier” for operational forces, it also becomes a critical vulnerability to those forces. At the same time, many current concepts and plans for operating in anti-access and area-denial environments depend on reliable access to cyberspace. However, some of the nations most able to deny allied forces access to an operational environment also may be able to deny access to the satellites currently underpinning access to cyber.

This paper proposes ensuring reliable access to cyber for command and control by developing operational procedures to utilize unmanned airborne relays. In addition the other operational benefits that would follow from the use of relays are examined, including a more credible deterrence capability and benefits to intelligence collection, reconnaissance, and tactical-level actions.

Introduction

The ability of an operational commander to protect their means of command and control (C2) has long been recognized as a critical requirement in the successful prosecution of warfare. Passwords have been used since antiquity to verify soldiers were under the command of a friendly commander.[1] In recent wars, militaries worried about things like communications security (COMSEC) in order to keep the enemy from knowing their orders, but also to keep the enemy from inserting false or contradictory orders into their own C2 channels. [2] According to Milan Vego, a researcher of military operations, "Failure to adequately protect one's command and control means loss of freedom to act, losing the initiative, and perhaps, in the end, dooming a military enterprise."[3]

Performing C2 with modern military forces is now increasingly tied up in the ability to utilize the domain of cyberspace. Cyber was once simply a "force multiplier" whose function and use could be handed off to a subordinate staff and tactical commanders. But that is no longer true. In fact, the J-3 of U.S. Cyber Command, Major General Williams, argues that "[s]ince cyberspace operations are *fundamental to success*, commanders cannot continue to run the risk of inappropriately delegating *key operational decisions* because they and their staffs lack an understanding of the domain"[4] (emphasis added).

Advancements in technology by peer nations mean that the ability to access cyberspace at the time and place where it is most needed can no longer be guaranteed to the operational commander by simply tasking their J-6. At the same time, access to cyber will be required for the operational commander

[1] William Smith, William Wayte, and George E. Marindin, eds., *A Dictionary of Greek and Roman Antiquities*, 3rd ed., vol. 1 (London: J. Murray, 1901), 377, http://books.google.com/books?id=Cu89AAAAYAAJ.

[2] As defined in Chairman, U.S. Joint Chiefs of Staff, *Joint Publication 6-0: Joint Communications System* (Washington, DC: CJCS, June 12, 2010), I-12

[3] Milan N. Vego, *Joint Operational Warfare: Theory and Practice*, rev. ed. (Newport, RI: Naval War College Press, September 20, 2007), VIII-54.

[4] Brett T. Williams, "The Joint Force Commander's Guide to Cyberspace Operations," *Joint Force Quarterly*, no. 73 (Second Quarter 2014): 12-13.

to overcome the increasing threat and proliferation of anti-access and area-denial (A2/AD) technologies.[5] This need for cyber, balanced with the risk to cyber access, means that *assured access into future opposed environments will require integrating theater level cyberspace capabilities into the joint task force's planning and operations*.

The ability for an operational force to establish an organic cyberspace access capability will also bring other advantages to the commander and their force. But before those are described, it is first necessary to establish why access to cyberspace is important to modern military operations.

Modern military operations rely on cyberspace

Cyberspace has become instrumental to the military due to several factors. However perhaps the most important reason was the requirement from the military services to increase their combat effectiveness in response to resource and budget pressures since the end of the Cold War.

Shrinking force levels

Take the U.S. Navy as an example. The Navy has long been facing a scenario of fewer and fewer major combatants to assign and allocate to the geographic combatant commands around the world. The current goal is to stabilize at 88 large surface combatants.[6] As an indication of the degree of the planning problem, the Navy's shipbuilding plan for fiscal year (FY) 2020 has dropped from 322 (in the FY 12 shipbuilding plan) to 304 in the FY 14 plan, a large change in just two years.[7] As a result each large surface combatant becomes correspondingly more precious, and this places a larger requirement on the survivability of such platforms.

[5] Chairman, U.S. Joint Chiefs of Staff, *Joint Operational Access Concept (JOAC)* (Washington, DC: CJCS, January 17, 2012), 9-10.

[6] Congressional Budget Office, *An Analysis of the Navy's Fiscal Year 2014 Shipbuilding Plan* (Congressional Budget Office, October 2013), 10, http://www.cbo.gov/publication/44655.

[7] Ronald O'Rourke, *Navy Force Structure and Shipbuilding Plans: Background and Issues for Congress* (Congressional Research Service, April 7, 2014), 11.

Another Navy response has been to focus on reduction in crew sizes to make ships cheaper to operate, and by rotating crews to get more deployed time out of fewer ships.[8] The recently-introduced Littoral Combat Ship (LCS) was designed for a crew of 40 (80 with full mission loadout[9]) as compared to a crew size of 215 for the *Oliver Hazard Perry* frigates LCS is intended to replace.[10] Similarly, the upcoming *Gerald R. Ford*-class aircraft carriers are intended to shave off a total of nearly 1,100 crew between the ship and its embarked air crew, with the capability gap to be filled by automation and cyber-enabled streamlining of administration. [11]

Deficiencies offset with cyber

The final step for the Navy in reducing crew sizes is to get the most marginal use out of each sailor by integrating combat functions in fewer (but more capable and more expensive) platforms. This integration was made possible by the fleet connectivity present in their task forces, and it supports the Navy's efforts to maximize the combat power of their fleets even as ship building budgets decrease.

However it leaves the naval forces more brittle—the Navy could experiment with these concepts when they could still fall back on specialized platforms if the network concept did not pan out. Now the specialized platforms are mostly gone (and the rest are disappearing fast) so network connectivity is *mandatory*—not simply a good idea—in order to ensure that naval platforms have mutual support from other naval and joint assets in a crisis.

Navy leadership recognizes this, and have been pushing to reshape the concept of operations for fleet warships to focus on cooperative engagement using real-time networking to regain the combat potential lost with decreasing fleet sizes. This represents the same concept (improvements of networked

[8] Thomas Rowden, "Operate Forward: LCS Brings It," *Navy Live: Official Blog of the United States Navy*, last modified May 3, 2014, http://navylive.dodlive.mil/2014/04/29/operate-forward-lcs-brings-it/.

[9] Christopher P. Cavas, "U.S. Navy Boosting LCS Core Crew Up to 50%," *Defense News*, last modified May 3, 2014, http://www.defensenews.com/article/20120702/DEFREG02/307020001/.

[10] U.S. Navy, *Cruisers, Destroyers & Frigates*, accessed May 4, 2014, http://www.navy.com/about/equipment/vessels/cruisers.html.

[11] U.S. Navy, *United States Navy Fact File: Aircraft Carriers - CVN*, last modified November 20, 2013, http://www.navy.mil/navydata/fact_print.asp?cid=4200&tid=200&ct=4.

warfighting and rapid shared understanding of the operational environment) that caused the development of the first digital networked fire control system, NTDS.[12] The broad implications of this capability have been discussed since 1997, and have even resulted in far-ranging planning assumptions for combatant design. [13] The LCS design concept of operations (CONOPS) relies on being part of "a networked battle force" particularly during "high threat environments."[14]

The reasoning is analogous to the way the Navy networks their fighter planes; the upcoming F-35C Joint Strike Fighter is even planned to be used to scout contested environments and use networked communications with an E-2D Advanced Hawkeye to share that information with the carrier strike group, while the U.S. Air Force employs similar capabilities. [15]

Those capabilities put in practice have been limited to tactical targeting and situational awareness purposes however; there is much less action (if more hot air) regarding the *operational*—not just administrative—implications of pervasive networked connectivity on the exercise of C2.

This is not for sheer lack of attention. For example Army officers have looked into networked command and control since before 1999, when the Army Battle Command System was analyzed to determine its suitability for its stated goal of increasing the commander's situational awareness. [16]

[12] David L. Boslaugh, "No Damned Computer is Going to Tell Me What to DO: The Story of the Naval Tactical Data System, NTDS," *IEEE First Hand Histories*:§ 1.3.2.1, accessed May 14, 2014, http://www.ieeeghn.org/wiki/index.php/First-Hand:No_Damned_Computer_is_Going_to_Tell_Me_What_to_DO_-_The_Story_of_the_Naval_Tactical_Data_System,_NTDS.

[13] Naval Surface Warfare Center Dahlgren Division (NSWC-DD), *Toward an Integrated Environment for Warfighting Control* (September 1997), 5.

[14] Ronald O'Rourke, *Navy Littoral Combat Ship (LCS) Program: Background, Issues, and Options for Congress* (Congressional Research Service, April 6, 2012), 19.

[15] Dave Majumdar, "Navy: F-35C Will Be Eyes and Ears of the Fleet," *USNI News*, last modified May 5, 2014, http://news.usni.org/2013/12/31/f-35c-will-eyes-ears-fleet.

[16] James D. Lee, "Information Dominance in Military Decision Making" (master's thesis, Army Command and General Staff College, 1999).

Rise of Cyber-enabled warfighting

The net effect of all this is a situation where fewer forces, manned by fewer personnel, rely increasingly on the cyber capabilities of their platforms for their combat effectiveness (i.e., cyber is needed for more than passing tactical targets to nearby forces). The Joint Force Commanders (JFCs) commanding these forces will also rely heavily on cyberspace to execute operational command and control. This need for cyber capability is certainly not limited to the Navy (or even any single service) alone: by the later stages of Operation ENDURING FREEDOM, carrier-based aircraft would take off for combat sorties without an assigned target—the target would be located and data sent while the plane was in the air, drastically shortening the time between positive identification and resultant fires.[17] Additionally F-14 Tomcats were able to share imagery intelligence with joint ground forces (especially special operations forces (SOF)).[18]

What this means for the operational commander is that access to cyber is a critical strength which must be protected to protect the force's center of gravity. Instead of having stovepiped communications means that cannot talk to each other, joint forces are converging on "cyber" as the way to not only communicate, but pass intelligence, analyze it, gain battlespace awareness, and more.

As a result, it is important for the JFC to understand the ways in which their force can be degraded by adversary attacks in the cyber domain, and what the JFC can do about it. Perhaps most important is moving past the idea that "cyber" is "communications." That is certainly true to a degree, but just as the Internet changed the face of civilian communications, so cyber has changed the face of C2. Cyber can provide communications, but also is an enabler or force multiplier for many more operational functions. But access to cyberspace is not guaranteed.

[17] Thomas P. Ehrhard and Robert O. Work, *Range, Persistence, Stealth, and Networking: The Case for a Carrier-Based Unmanned Combat Air System* (Washington, DC: Center for Strategic and Budgetary Assessments, 2008), 105.

[18] Ibid., 105.

Cyberspace is vulnerable to disruption

The last section has demonstrated the importance of cyber to the operational level of modern war. Like other revolutionary military technologies, the advantages of cyber are also accompanied by areas of concern.

For instance, cyber is only useful to a force if that force can gain access to it (and more specifically, access to the same cyberspace that the rest of the force has presence in).

Access to cyber can come over many different carriers, including line-of-sight (LOS) electromagnetic (EM) beams, satellite connections, physical connections (such as fiber optics or Ethernet cabling), and even more. In the military context, physical connections to allied cyberspace are difficult to come by in enemy territory, which leaves LOS connections or satellite as the primary access to cyber.

Both of these means have issues that must be considered at the operational level, not just the tactical level. For instance, LOS capabilities are short-ranged at ground level (range through the air is longer), and since they involve EM radiation, also have operations security (OPSEC) concerns. They are highly-demanded resources, which require operational level planning to match means to ends most effectively while allowing for decentralized execution.

Issues with LOS access

Wireless communication of signals almost always involves some form of EM radiation (such as radio waves or light) being sent from a transmitter to a receiver. In fact, one of the oldest long-range communications of antiquity (signal towers using torches) can be considered EM-based LOS wireless communication. [19]

[19] Herodotus, *History*, trans. G. C. Macaulay, vol. 2 (1890), book 7, ¶ 183.

EM communications can be jammed by EM signals, and they normally require a clear path from the sender to the receiver. [20] Unless directional antennas and receivers are used the power requirement for the transmitter can be substantial as well. Additionally the careless use of EM can give away a unit's position unless special measures are taken to reduce their detectability (LPI technologies, which refer to their low probability of interception).[21]

All of these issues have practical counter-measures with modern communications systems such as Link 11 and Link 16, which are long range (when using long-haul protocols) and resistant to jamming. However, these data links are stovepiped to limit communications to tactical needs. They are suitable for fire control and coarse awareness of the operational environment, but have only limited voice capacity and access to the cyber capabilities needed for intelligence sharing. In addition, they require dedicated track management to ensure a shared understanding of the operational environment, which adds the requirement for a Force Track Coordinator in the Navy's Composite Warfare Concept.[22]

Issues with access to space

In order to get full access to cyber space with mobile units, joint forces have been tremendously reliant on space-based assets to relay the needed communications to access cyber.

Space-based relays are still LOS connections, with all the same failings. However satellites are in practice even more susceptible to the possibility of jamming, which would be bad enough: U.S. Central Command alone developed an emergent requirement for more than 15 million bits per second at the

[20] Brien Alkire et al., *Applications for Navy Unmanned Aircraft Systems* Monograph no. MG-957-NAVY (Santa Monica, CA: RAND, 2010), 28; Some over-the-horizon signals are possible with techniques like HF radio, but these are less reliable.

[21] Jonathan F. Solomon, "Maritime Deception and Concealment: Concepts for Defeating Wide-Area Oceanic Surveillance-Reconnaissance-Strike Networks," *Naval War College Review* (Newport, RI) 66, no. 4 (Autumn 2013): 89.

[22] Paul T. Mitchell, "Small Navies and Network-Centric Warfare: Is There a Role?," *Naval War College Review* (Newport, RI) LVI, no. 2 (Spring 2003): 85; Chief of Naval Operations, *Composite Warfare Doctrine*, Navy Warfare Publication (NWP) 3-56 (Washington, DC: Department of the Navy, CNO, September 2010), 5-5.

beginning of Operation ENDURING FREEDOM, when many U.S. households were capable of less than one-thousandth that amount. That requirement was provided by space-based capabilities.[23]

However some nations now have the ability to destroy or disable satellites outright with anti-satellite (ASAT) technology, forcing the combatant commander to analyze the problem of how to provide cyber without space.[24] Even if the JFC would like to assume that an ASAT-capable nation would not use this ability during an armed conflict, there is an inherent escalation dominance concern that is a political issue and would be resolved at the highest levels of government.

Such a scenario could lead to political leadership imposing controls on the military as has happened in previous conflicts. For example, one can imagine a ban on using civilian space assets for military purposes (perhaps with limited exceptions) during an armed conflict, in exchange for guarantees from the adversary not to utilize ASAT first. This would severely hamper the operational commander's ability to utilize cyber unless the JFC can integrate other means.

While a full discussion of deterrence concerns is beyond the scope of this short paper, it suffices to mention that for the near future the U.S., as a global power, will have more (and probably far more) to lose from loss of access to both space and cyber than almost any possible adversary. This makes it difficult to use "eye for an eye" deterrence methods to prevent an adversary using ASAT, which means the JFC must plan to not have space available, and therefore, cyber through space.

Luckily, many of the force assets that will be available to JFCs in 2020 can be used (or easily converted) to provide organic unit ability to access cyber and help protect C2.

[23] Ehrhard and Work, *Range, Persistence, Stealth, and Networking*, 105.

[24] Vincent Alcazar, "Crisis Management and the Anti-Access/Area Denial Problem," *Strategic Studies Quarterly* (Maxwell AFB, AL) 6, no. 4 (Winter 2012): 44.

Future JTFs can organically provision cyberspace

As it turns out, the state of the art for access to cyberspace has advanced significantly since the first wireless computer network was implemented in 1970.[25]

Wireless access to cyberspace is nearly ubiquitous, even in developing countries. Moreover, wireless connections have grown more advanced since 1970—even many "backhaul" Internet connections are made via wireless relay connections when initially servicing an area, even though it would be perfectly feasible to run fiber optic cabling.[26] So the difficulty with access to cyber in an ASAT environment is not the need to use wireless, it is the need to use wireless beyond the LOS of the unit needing access to cyber (which can be out to sea far past friendly shores).

This is where the ability to use unmanned aerial vehicles (UAVs) plays in. It does not take much ingenuity to figure out that a UAV (which can continuously reposition itself) can replace a satellite (which operates in an orbit that is fairly easy to predict a position from). Indeed, the communications relay mission has been studied extensively and discussed widely in the literature.[27] This is unsurprising, since without some other ability to communicate to and from a UAV, these assets are completely dependent upon satellite availability—leaving the operational commander not just without satellite, but without their best ISR platform unless countermeasures are developed.[28]

By using a relay of UAVs carrying communications gear, access to cyberspace can be assured at just the locations where it is needed, only at the time it is needed, allowing the JFC to "bring their own cyber access", a concept that will be referred to as BYOCA throughout this paper. This communications

[25] Norman Abramson, "THE ALOHA SYSTEM: Another Alternative for Computer Communications," in *Proceedings of the November 17-19, 1970, Fall Joint Computer Conference*, AFIPS '70 (Fall) (Houston, Texas: ACM, 1970), 281.

[26] Laetitia Garriott de Cayeux, "The Future of Wireless is Wired," *Forbes* (April 1, 2012), last modified April 1, 2012, http://www.forbes.com/sites/techonomy/2012/04/01/the-future-of-wireless-is-wired/.

[27] e.g. in Solomon, "Maritime Deception and Concealment," 89; Ehrhard and Work, *Range, Persistence, Stealth, and Networking,* 217; and Alkire et al., *Applications for Navy Unmanned Aircraft Systems*, xvi.

[28] Alkire et al., *Applications for Navy Unmanned Aircraft Systems*, 28.

gear will support LPI to enable low-signature (and high OPSEC) use, and can be configured to make jamming nearly impossible.[29]

In addition, the UAVs necessary can be carried by multiple types of surface combatants (and if near enough to friendly shores, need not be carried by naval assets at all). [30] This capability would also permit UAVs operating in denied environments to quickly pass the intelligence data being collected back to analysis cells in a safer area for *real-time* analysis and cueing, without necessarily alerting the adversary to what is going on.

Counterarguments to the proposed need for organic cyber

There are several possible critiques of this approach, the most important of which include:

Prioritization of UAV Functions: By using UAVs to perform relay to cyberspace, it is that much more difficult to use each UAV so assigned for other important missions. This can be mitigated somewhat by the possibility of assigning UAVs in a "relay orbit" to other tasks such as maritime surveillance of opportunity, operating a search radar in a scenario where deception concerns forbid a unit using their own radar, etc. In addition surface units could also participate in the relay (including concealed craft) between two UAVs out of each other's LOS to reduce the number of required UAVs.

But the issue remains, especially if the UAVs required to support this mission are in short supply, as this would necessitate the JFC having to decide for each tactical action which risks to accept in allocating missions to a finite force, much like Adm. Nagumo deciding between reconnaissance, attack, and combat air patrol before the Battle of Midway.

Backup plans are still required: UAVs can suffer equipment failure while on station, be shot down by the adversary, or experience any number of other hardships that cause the UAV to become a mission failure. Because of this there should still be provision for loss of access to cyber. What that would mean during any given operation must be decided by the operational commander. For one mission, access

[29] Alkire et al., *Applications for Navy Unmanned Aircraft Systems*, 36.
[30] Ibid., 51,53.

to cyber might be so vital that redundant relays are emplaced for the mission, while on another mission the risk of loss of access might be acceptable past a certain point in the operation.

Complexity: It is undeniable that a plan to assure access to cyber by relaying communications through UAVs of different types, using methods of different types, to connect to endpoints of even more types is complex on its own, in the very area argued to be increasingly important for mission success. In fact a 2010 study of existing Navy networks showed that 50% of networked technology failures stem from an underlying cause of human error.[31] While these mission networks would not be more complicated than shipboard networks (not to mention those on shore), it is clear that a good deal of training and institutional knowledge would be needed to ensure a given probability of success.

Despite these issues, the core idea is workable even without space, allowing the JFC to get the benefits of cyber in their effort towards meeting their objective. The issues do mean that the JFC must be aware of the risks, in order to make the best possible decision, but assuming the pervasive ability to access cyber is provided, there are other advantages that the operational commander would gain.

Organic cyberspace can give operational advantages

Perhaps the biggest advantage towards meeting the Joint Operational Access Concept (JOAC) is that cyber-based C2 allows for the usage of much smaller and much less expensive platforms, to act as both sensors and as payload-delivery platforms. [32] One of the biggest problems of the "anti-access" issue is that in many ways the issue is self-imposed: A rational commander would not send a very expensive and massively advanced platform into harm's way, unless the value of the operational objective warrants the incredible risk to that platform. [33] The required value of an objective needed in order to task a platform to accomplish that objective increases as the cost of the platform itself increases; very expensive

[31] Isaac R. Porche III et al., *Navy Network Dependability: Models, Metrics, and Tools* Monograph no. MG-1003-NAVY (Santa Monica, CA: RAND, 2010), xvii.

[32] Chairman, U.S. Joint Chiefs of Staff, *Joint Operational Access Concept (JOAC)*.

[33] DDG-51 warships now cost $1,484.7 million according to Ronald O'Rourke, *Navy DDG-51 and DDG-1000 Destroyer Programs: Background and Issues for Congress* (Congressional Research Service, April 8, 2014), 21.

platforms end up being reserved to accomplish only the most essential and demanding tasks, leaving an "objective gap" of tasks that are important, but not important enough to accept the risk necessary to accomplish it with a high-value platform.

Better balance between risk and reward

Smaller and cheaper craft can accept higher risk, but have been, up to now, much less capable than high-end platforms with advanced weapons and sensors. The situation would change if the JFC were provided an inexpensive platform with an inexpensive surface search radar, and allowed it to penetrate deeply into the threat zone. By letting it get very close the short range of the radar is no longer an issue. The short range might even turn into an advantage, as such a platform would be more difficult to detect by electronic sensors in range of the low-powered beam. Protection for the craft can be ensured by blending into surface traffic, and if deception fails and the radar picket ship gets attacked, there is much less of a crisis if the ship is hit. The fruit of this labor can be instantly delivered over the covertly-formed cyber network, not only to the Joint Force Headquarters (JFHQ), but to *all allied forces on the network*.

Alternately, if the JFC could split the *defensive* tasks assigned to an allied ship away to a different unit, that ship could be freed up to carry out *offensive*, close-in tasks, without placing the Joint Force in a defenseless position. For instance, the high-powered radar for the air defense role normally handled by AEGIS-equipped warships could be shifted to a dedicated "Sea-WACS".[34] Of course, this is already mostly possible with Link 11—the point is that the JFC will be able to apply the same principles to other assets that share capabilities (and access to cyber) where the loss of one would be less risky than the other.

At the other end of the spectrum, it is not hard to imagine a "gunboat" mission module for LCS that brings the payload needed for operational and tactical fires. Other low-signature assets such as guided missile nuclear submarines (SSGNs) or *Virginia*-class nuclear submarines with a Virginia Payload

[34] O'Rourke, *Navy DDG-51 and DDG-1000 Destroyer Programs*, 17.

Module (VPM) could also be used. These assets would provide the payload but not perform the targeting—this would be provided by separate assets (e.g. the mentioned radar pickets, UAVs performing reconnaissance, etc.). Since these assets would not be emitting on their own tactical sensors the ability to deceive the adversary about the threat present in the operational environment is greatly increased, which would thereby strain their decision calculus. This becomes possible when the operational commander can logically split the *sensor platform* from the *payload platform* and share the best sensor data to the platform that can best utilize it.[35]

This would all rely on having the needed tactical system data links, a shared, real-time understanding of the operational environment, and a willingness to allow the tactical commanders to meet the JFC's intent in the best way possible at the tactical level. Operational access to cyberspace can provide this, by providing a superior platform for C2, analogously to the way Link 11 and Link 16 datalinks provide tactical-level rewards in the Navy's Cooperative Engagement Capability program.[36]

Improved intelligence & planning support

Another advantage that can result from the BYOCA concept is regaining the ability to perform detailed intelligence, surveillance and reconnaissance (ISR) in contested and denied areas, at lower risk and cost. This is another area of concern to strategic and operational planners; despite the key importance of good intelligence to the operational commander who must gain access to an A2/AD operational environment, current thinking about intelligence in this scenario is still unrefined, even though the threat of A2/AD technologies has been discussed since 1997.[37]

The same UAVs that are performing the relay function for BYOCA can usually be used to perform ISR functions as well. Alternately, the need for ISR alone might justify sending UAVs aloft into

[35] NSWC-DD, *Toward an Integrated Environment for Warfighting Control*, 18.

[36] Mitchell, "Small Navies and Network-Centric Warfare," 86.

[37] Andrew Robert Marvin, "ISR Support to Operational Access: Winning Initiative in Antiaccess and Area-denial Environments," *Joint Force Quarterly*, no. 71 (Fourth Quarter 2013): 54; NSWC-DD, *Toward an Integrated Environment for Warfighting Control*, 5.

contested and denied areas—without a system like BYOCA to send the data back to a fusion center, there would be no way to act on this data in real time in a denied-space scenario, and this would greatly increase the risk that the ISR platform would be destroyed before it could return with the needed information. It is even conceivable to send a penetrating UAV to gain forcible entry to the adversary's cyber space.[38]

Additionally, the BYOCA concept would provide the cyber substrate needed to allow for the best operational planning products from the joint forces who increasingly perform their planning using virtualization and remote-access, which requires increasingly capable cyber access to succeed.[39]

Tactical Improvement

Combining data flow, quick command and control reach-back, and real-time voice communications at a tactical level can allow for incredibly short observation-action timelines, and a possibility of actually achieving the "cross-domain synergy" advertised in the JOAC.[40] This can all happen without space capability, and even if space is available, using a "only the links we need" network can help mitigate the risk of the adversary using offensive network operations to read friendly communications traffic as it passes over satellite.

At the same time, multiplying the number of forces that can be sent to the theater of operations greatly strains the adversary's ability to make good, quick decisions. If they launch antiship cruise missiles (ASCM) against friendly small craft or other decoys, they risk giving away the location of their

[38] David A. Fulghum, "Navy Pushes Cyber Options," *Aviation Week & Space Technology* 172, no. 13 (March 29, 2010): 2nd paragraph.

[39] John P. Looney and Mark E. Nissen, "Computational Modeling and Analysis of Networked Organizational Planning in a Coalition Maritime Strike Environment" (student paper, presented at 2006 Command and Control Research and Technology Symposium, Monterey, CA, 2006), 20, available as Defense Technical Information Center (DTIC) Report ADA463314.

[40] Lee, "Information Dominance in Military Decision Making," 3, 55, 73, 78; NSWC-DD, *Toward an Integrated Environment for Warfighting Control*, 11; Chairman, U.S. Joint Chiefs of Staff, *Joint Operational Access Concept (JOAC),* ii.

mobile launchers and wasting possibly valuable ordnance.[41] If they do not launch then they risk allowing the JFC to gain a much better situational awareness of the operating environment, or even allowing the JFC to use operational fires to shape the battlespace in favor of allied forces.

This type of swarm capability is not far off, either: The ability for UAVs linked by a cyber network to cooperatively attack emergent targets has already been demonstrated, and studies of the combat effectiveness of "surface swarms" demonstrate a cost-effective (and far less brittle) way to achieve operational effects from cooperative forces, even without allowing the swarm to communicate with each other.[42]

The possible applications of this capability are in many ways bounded only by the imagination of the operational commander and their staff, and the tactical commanders who would be on the front lines. But it all rests on the substrate of real-time intelligence sharing, communications, and C2, which itself can best be provided by a secure cyber ability. And it requires decisions on the part of the operational commander, since the best cyber-enabled C2 model may vary, which leaves the JFCs (and their JFMCC) with a choice to make. [43] At the same time, the necessary elements of how command would be exercised would still belong to the JFC (and their JFMCC), which would necessitate operational-level planning on how to exercise this type of warfare tactically.[44]

Conclusion

Budget pressures and the unique post-Cold War security environment combined to lead the Navy toward a path of combining mission sets for their surface combatants into fewer but more capable (and

[41] Solomon, "Maritime Deception and Concealment," 95.

[42] Ehrhard and Work, *Range, Persistence, Stealth, and Networking*, 127; Jimmy Drennan, "Strength in Numbers: The Remarkable Potential of (Really) Small Combatants," *Naval War College Review* (Newport, RI) 67, no. 1 (Winter 2014): 129.

[43] Looney and Nissen, "Computational Modeling and Analysis of Networked Organizational Planning in a Coalition Maritime Strike Environment," 18.

[44] Robin N. Keister, "Designing the Joint Force Maritime Component Commander Through Practical Applications Past, Present and Future" (strategy research paper, U.S. Army War College, Carlisle Barracks, PA, April 15, 2002), 17.

more expensive) combatants, filled with advanced technology and crewed by highly-trained sailors. These fleets were then made even more capable by networked battle concepts, but this added a new critical vulnerability by underpinning combat power on access to cyber.

The proliferation of anti-ship cruise and ballistic missiles has lead to a much different operational environment for the Navy's surface combatants in many possible future combat theaters. These A2/AD technologies push the safe operating range of expensive surface combatants (and possibly even submarines) far from where they will be needed.

At the same time, new abilities for potential adversaries to attack the friendly ability to access cyber have cropped up in parallel, especially in space, which would put the ability of forces to conduct networked battle at risk, and leave them liable to defeat in detail.

The JFC in 2020 will have the ability to counter threats to his cyber access by the inventive use of assigned forces. Doing this will necessarily involve prioritizing against other possible missions for these forces, and cannot be pushed down to just the J-6. In fact, forcing access to cyber as a prelude to forcible access to the assigned operating areas will involve changes to the entire CONOPS, along with cooperation between the elements of the JFC's staff to ensure and best utilize this access to cyber space.

However, this altered CONOPS will also buy the opportunity to utilize networked battle at a much lower (and more capable) tactical level. For the first time since World War II, the U.S. and allied forces might be able to employ "counter-swarm" tactics at acceptable risk based on the C2 capabilities provided by pervasive and secure access to cyber.

Perhaps more importantly, demonstrating the ability to fight and win in degraded environments has a deterrent effect all its own—if possible adversaries can be convinced that they could not credibly defeat allied forces even with attacks on allied C2, they would be that much less willing to risk defeat by trying.

However, like with any major change to the doctrine of a large institution, the changes that would be needed to spell out this concept to the actionable level cannot be planned out in just a week. JFCs would need to take early action to determine the possible risk to cyber access in their particular assigned areas, the feasibility of using these concepts with forces assigned, and simulations and training to determine the best tactics, techniques and procedures to use.

Despite the work that would be needed, taking these actions to assure access to cyberspace for command and control is vital to ensuring that America retains the ability to access the global commons in support of national interests, forcibly if necessary.

Recommendations

Geographic Combatant Commanders and their subordinate Joint Force Commanders should start planning on how to use forces assigned in degraded-space environments in a way that still maximizes their effectiveness. Concepts such as "mission command" and "command by negation" have been used successfully by militaries in the past in such environments. However these concepts have not normally been been aided by pervasive tactical-level information sharing as would be possible with BYOCA. Additionally these concepts, if left unmodified, leave out the possibility of quick reach-back to the operational commander. JFCs should examine the possibilities of combining low-comms concepts with pervasive cyber access.

One other important implication for the JFC which remains mostly undiscussed in this paper, is the importance of prioritizing access to cyber communications amongst subordinate units should the demand for data throughput exceed the capacity of a degraded cyber system to carry. In such a scenario having clear priorities on what data the JFC needs most urgently is the only way to ensure that important information is not inadvertently prevented from being sent to where it is needed most.[45]

Friendly "think tanks" and service colleges should assist by coming up with the implications and possible uses of this deep immersion into cyber access, and war gaming them to see how they can best be

[45] E.g. during the Apollo 11 mission an unexpected radar/computer interaction during lunar landing was prevented from turning disastrous only by the foresight to have the computer prioritize running programs in case of CPU contention.

employed. It might turn up that emergent behaviors pop out that can be utilized for operational functions, or even that what appears to be a good idea on paper ends up being impracticable in practice.

Other useful applications are undoubtedly available to the operational and tactical commanders as well. For instance it might be useful to “park” a UAV in a known orbit for submarines to communicate with in order to clear their broadcast in a denied-space scenario. This is a capability not available in a “dumb” relay that cannot store data, or hover in place waiting for the other party. Military research labs and systems commands could engage in developing other applications.

Finally (and unfortunately) the need to plan for mitigation strategies in a counter space scenario is not fully solved even using this plan. UAVs will not provide GPS fixes so having backup strategies for wartime communication, navigation, etc. are still useful—but these backup strategies will be usually service-specific or tactically driven, unlike the possibilities of pervasive integrated cyber.

Bibliography

Abramson, Norman. "THE ALOHA SYSTEM: Another Alternative for Computer Communications." In *Proceedings of the November 17-19, 1970, Fall Joint Computer Conference*, 281–285. AFIPS '70 (Fall). Houston, Texas: ACM, 1970. doi:10.1145/1478462.1478502.

Alcazar, Vincent. "Crisis Management and the Anti-Access/Area Denial Problem." *Strategic Studies Quarterly* (Maxwell AFB, AL) 6, no. 4 (Winter 2012): 42–70.

Alkire, Brien, James G. Kallimani, Peter A. Wilson, and Louis R. Moore. *Applications for Navy Unmanned Aircraft Systems* Monograph no. MG-957-NAVY. Santa Monica, CA: RAND, 2010.

Boslaugh, David L. "No Damned Computer is Going to Tell Me What to DO: The Story of the Naval Tactical Data System, NTDS," *IEEE First Hand Histories*. Accessed May 14, 2014. http://www.ieeeghn.org/wiki/index.php/First-Hand:No_Damned_Computer_is_Going_to_Tell_Me_What_to_DO_-_The_Story_of_the_Naval_Tactical_Data_System,_NTDS.

Cavas, Christopher P. "U.S. Navy Boosting LCS Core Crew Up to 50%." *Defense News*. Last modified May 3, 2014. http ://www.defensenews.com/article/20120702/DEFREG02/307020001/.

Congressional Budget Office. *An Analysis of the Navy's Fiscal Year 2014 Shipbuilding Plan*. Congressional Budget Office, October 2013. http://www.cbo.gov/publication/44655.

de Cayeux, Laetitia Garriott. "The Future of Wireless is Wired." *Forbes* (April 1, 2012). Last modified April 1, 2012. http://www.forbes.com/sites/techonomy/2012/04/01/the-future-ofwireless-is-wired/.

Drennan, Jimmy. "Strength in Numbers: The Remarkable Potential of (Really) Small Combatants." *Naval War College Review* (Newport, RI) 67, no. 1 (Winter 2014): 125–134.

Ehrhard, Thomas P., and Robert O. Work. *Range, Persistence, Stealth, and Networking: The Case for a Carrier-Based Unmanned Combat Air System*. Washington, DC: Center for Strategic and Budgetary Assessments, 2008.

Fulghum, David A. "Navy Pushes Cyber Options." *Aviation Week & Space Technology* 172, no. 13 (March 29, 2010): 61.

Herodotus. *History*. Translated by G. C. Macaulay. 1890.

Keister, Robin N. "Designing the Joint Force Maritime Component Commander Through Practical Applications Past, Present and Future." Strategy research paper, U.S. Army War College, Carlisle Barracks, PA, April 15, 2002.

Lee, James D. "Information Dominance in Military Decision Making." Master's thesis, Army Command and General Staff College, 1999.

Looney, John P., and Mark E. Nissen. "Computational Modeling and Analysis of Networked Organizational Planning in a Coalition Maritime Strike Environment." Student paper, presented at 2006 Command and Control Research and Technology Symposium, Monterey, CA, 2006.

Majumdar, Dave. "Navy: F-35C Will Be Eyes and Ears of the Fleet." *USNI News*. Last modified May 5, 2014. http://news.usni.org/2013/12/31/f-35c-will-eyes-ears-fleet.

Marvin, Andrew Robert. "ISR Support to Operational Access: Winning Initiative in Antiaccess and Area-denial Environments." *Joint Force Quarterly*, no. 71 (Fourth Quarter 2013): 53–57.

Mitchell, Paul T. "Small Navies and Network-Centric Warfare: Is There a Role?" *Naval War College Review* (Newport, RI) LVI, no. 2 (Spring 2003).

Naval Surface Warfare Center Dahlgren Division (NSWC-DD). *Toward an Integrated Environment for Warfighting Control*. September 1997.

O'Rourke, Ronald. *Navy DDG-51 and DDG-1000 Destroyer Programs: Background and Issues for Congress*. Congressional Research Service, April 8, 2014.

________ , *Navy Force Structure and Shipbuilding Plans: Background and Issues for Congress*. Congressional Research Service, April 7, 2014.

________ , *Navy Littoral Combat Ship (LCS) Program: Background, Issues, and Options for Congress*. Congressional Research Service, April 6, 2012.

Porche III, Isaac R., Katherine Comanor, Bradley Wilson, Matthew J. Schneider, Juan Montelibano, and Jeff Rothenberg. *Navy Network Dependability: Models, Metrics, and Tools* Monograph no. MG-1003-NAVY. Santa Monica, CA: RAND, 2010.

Rowden, Thomas. "Operate Forward: LCS Brings It." *Navy Live: Official Blog of the United States Navy*. Last modified May 3, 2014. http://navylive.dodlive.mil/2014/04/29/operateforward-lcs-brings-it/.

Smith, William, William Wayte, and George E. Marindin, eds. *A Dictionary of Greek and Roman Antiquities*. 3rd ed. London: J. Murray, 1901. http://books.google.com/books?id=Cu89AAAAYAAJ.

Solomon, Jonathan F. "Maritime Deception and Concealment: Concepts for Defeating Wide-Area Oceanic Surveillance-Reconnaissance-Strike Networks." *Naval War College Review* (Newport, RI) 66, no. 4 (Autumn 2013): 87–116.

U.S. Navy. *Cruisers, Destroyers & Frigates*. Accessed May 4, 2014. http://www.navy.com/about/equipment/vessels/cruisers.html.

________ , *United States Navy Fact File: Aircraft Carriers - CVN*. Last modified November 20, 2013. http://www.navy.mil/navydata/fact_print.asp?cid=4200&tid=200&ct=4.

U.S. Navy. Office of the Chief of Naval Operations. *Composite Warfare Doctrine*. Navy Warfare Publication (NWP) 3-56. Washington, DC: Department of the Navy, CNO, September 2010.

U.S. Office of the Chairman of the Joint Chiefs of Staff. *Joint Operational Access Concept (JOAC)*. Washington, DC: CJCS, January 17, 2012.

________ , *Joint Publication 6-0: Joint Communications System*. Washington, DC: CJCS, June 12, 2010.

Vego, Milan N. *Joint Operational Warfare: Theory and Practice*. Rev. ed. Newport, RI: Naval War College Press, September 20, 2007.

Williams, Brett T. “The Joint Force Commander’s Guide to Cyberspace Operations.” *Joint Force Quarterly*, no. 73 (Second Quarter 2014): 12–19.